原議保存期間５年
（平成30年３月31日まで保存）

警察庁丁備企発第108号
平成24年５月30日
警察庁警備局警備企画課長

警視庁公安部長
各道府県警察本部長
殿
（参考送付先）
各警察情報通信部長
各管区警察局広域調整担当部長
各管区警察局情報通信部長
各府県（方面）情報通信部長
警視庁総務部長

情報収集用端末運用管理要領の制定について（通達）

このたび、情報収集用端末を全国の都道府県警察本部に整備したことに伴い、別添のとおり「情報収集用端末運用管理要領」を制定することとしたので、事務処理上遺漏のないようにされたい。

別添

情報収集用端末運用管理要領

1　目的

この要領は、情報収集用端末の運用管理に関する基本的事項を定めることにより、情報収集用端末の効率的かつ適切な運用を図ることを目的とする。

2　運用管理体制

(1) 総括責任者

ア　警察庁に情報収集用端末の総括責任者を置き、警察庁警備局警備企画課長をもって充てる。

イ　総括責任者は、情報収集用端末の運用管理を総括する。

(2) 運用管理者

ア　警察庁及び都道府県警察の情報収集用端末を利用する課に、運用管理者を置き、それぞれ当該課の長をもって充てる。

イ　運用管理者は、当該課における情報収集用端末の運用管理を行う。

(3) 運用管理補助者

ア　運用管理者は、当該課の課長補佐又は係長の職にある者の中から運用管理補助者を指定するものとする。

イ　運用管理補助者は、３に規定する事務に関し、運用管理者を補佐する。

3　運用管理者が講ずる措置

運用管理者は、次に定める措置を講じ、情報収集用端末を適切に管理しなければならない。

なお、当該端末の運用管理に当たっては、取扱説明書に従って作業を行うこと。

(1) 紛失、盗難等防止対策の実施

情報収集用端末に付属のセキュリティワイヤーを取り付け、当該端末の紛失、盗難及び設置場所からの不正な持ち出しを防止するための措置を講じなければならない。

(2) 不正プログラム対策の実施

次に定める措置を講じることなどにより、情報収集用端末の不正プログラム感染の予防に努めなければならない。

ア　情報収集用端末に付属のウイルス対策ソフトを導入し、管理者権限で情報収集用端末を操作することにより、常に当該ソフトウェアを最新の状態に維持するとともに、定期的に不正プログラムの検査を実施しなければならない。また、情報収集用端末に導入したオペレーションシステム及びその他のソフトウェアについても、常に最新の状態に維持しなければならない。

イ　情報収集用端末に付属の環境復元ソフトを導入し、当該端末の起動時にソフトウ

ェア等の設定が所定の状態に復元する機能を有効にしなければならない。

(3) 外部記録媒体の利用制限

付属の環境復元ソフトの機能を用いて、職員が許可なく外部記録媒体を利用して情報を入出力できないようにするための措置を講じなければならない。ただし、付属のソフトを用いず、都道府県警察において利用している別のソフトの機能等を用いて同様の措置を講じることを妨げない。

(4) アクセス権の付与、抹消等

ア　課の職員及びサイバーテロ対策プロジェクト要員等に情報収集用端末を利用させる必要があると認める場合は、当該職員（以下「利用職員」という。）に対して個別にアクセス権を付与するものとする。

イ　利用職員が４に定める措置を講じ、情報収集用端末を適切に管理するよう、利用職員に対し、必要な指導を行わなければならない。

ウ　情報収集用端末を利用させる必要がなくなった場合は、利用職員のアクセス権を抹消しなければならない。

(5) 取扱説明書の管理

取扱説明書の名称、受領及び返却の年月日、保管場所、廃棄方法等その他の状況を簿冊に記載し、保管庫等に保管しなければならない。

４　利用職員が講ずる措置

利用職員は、次に定める措置を講じ、情報収集用端末を適切に管理しなければならない。

(1) 警察情報の保存

当該端末に警察情報を含むファイルを保存したままにしてはならない。

(2) 情報収集用端末の持ち出し

情報収集用端末を警察機関の庁舎外へ持ち出す必要がある場合には、持ち出し期間を明らかにし、運用管理者の許可を得なければならない。また、庁舎外に持ち出すことを終了した場合には、運用管理者に対して、その旨を報告しなければならない。

(3) 不正プログラム対策の実施

不正プログラムに感染するおそれのあるウェブサイトを閲覧した場合には、コンピュータ・ウイルス対策ソフトによる検査を実施するなどにより、情報収集用端末の不正プログラム感染の予防に努めなければならない。

５　特異事案発生時の措置

(1) 運用管理者に対する報告

利用職員は、情報収集用端末の不正プログラム感染事案及び当該端末に対するサイバー攻撃事案等の特異事案の発生を認知した場合は、被害の拡大防止のため、当該端末を電気通信回線から切り離すなどの被害拡大防止措置を講じた上で、運用管理者に

速やかにその概要を報告しなければならない。

(2) 総括責任者に対する報告

運用管理者は、報告を受けた特異事案について、総括責任者に速やかに報告しなければならない。

6　その他の情報セキュリティ

その他の情報セキュリティに関して実施する運用管理対策、物理的対策、技術的対策その他の事項については、「警察情報セキュリティに関する訓令」（平成15年警察庁訓令第３号)、「警察情報セキュリティ対策基準」（平成22年３月30日付け警察庁丙情管発第72号、丙通施発第３号、丙総発第19号、丙生企発第54号、丙刑企発第47号、丙企分発第９号、丙交企発第58号、丙備企発第30号、丙外事発第19号別添）を始めとする警察情報セキュリティポリシーの定めるところによる。